

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 5月 8日

出 願 番 号

Application Number:

特願2001-136827

出 願 人

Applicant(s):

株式会社日立製作所

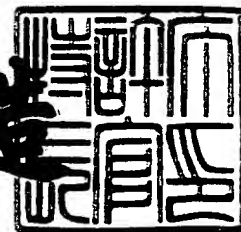
CERTIFIED COPY OF
PRIORITY DOCUMENT

USSN 09/940,594
MATTINGLY, STANGER, MALUR + BRUNDIDGE
(703) 684-1120
ASA-1029

2001年 8月31日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3077490

【書類名】 特許願

【整理番号】 K01000831A

【あて先】 特許庁長官

【国際特許分類】 G06F 17/60

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 富田 民則

【発明者】

 【住所又は居所】 東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所 公共システム事業部内

 【氏名】 宮崎 豊

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタル署名検証装置

【特許請求の範囲】

【請求項 1】

少なくともその一部にデジタル署名が施された部分データを含むデジタル署名データを入力するデジタル署名検証装置において、

前記デジタル署名データを入力する手段と、

前記デジタル署名データに含まれる、前記部分データの範囲を識別する識別子に基づいて、前記部分データの範囲を検知する手段と、

検知された前記部分データの内容を表示する手段とを有することを特徴とするデジタル署名検証装置。

【請求項 2】

請求項 1 に記載のデジタル署名検証装置において、

入力された前記デジタル署名データに施されたデジタル署名に関する情報を検出する手段を、さらに有し、

前記表示する手段は、検出された前記デジタル署名に関する情報を表示することを特徴とするデジタル署名検証装置。

【請求項 3】

請求項 2 に記載のデジタル署名検証装置において、

前記デジタル署名に関する情報は、前記デジタル署名を施した主体に関する情報であることを特徴とするデジタル署名検証装置。

【請求項 4】

請求項 2 または 3 のいずれかに記載のデジタル署名検証装置において、

前記表示する手段は、前記部分データの内容と前記デジタル署名に関する情報を関連付けて表示することを特徴とするデジタル署名検証装置。

【請求項 5】

請求項 4 に記載のデジタル署名検証装置において、

前記表示する手段は、前記部分データの内容を示す情報を他の情報と区別して表示することを特徴とするデジタル署名検証装置。

【請求項 6】

請求項 1 乃至 5 のいずれかに記載のデジタル署名検証装置において、

前記デジタル署名は、XML により記述され、

前記検知する手段は、所定のデータを指し示すものであって、XML により規定された前記識別子を検索し、検索された前記識別子に基づいて検知することを特徴とするデジタル署名検証装置。

【請求項 7】

コンピュータに対して、

少なくともその一部にデジタル署名が施された部分データを含むデジタル署名データを入力する機能と、

前記デジタル署名データに含まれる、前記部分データの範囲を識別する識別子に基づいて、前記部分データの範囲を検知する機能と、

検知された前記部分データの内容を表示する機能を実行させるコンピュータプログラム。

【請求項 8】

請求項 7 に記載のコンピュータプログラムにおいて、

入力された前記デジタル署名データに施されたデジタル署名に関する情報を検出する機能を、さらに前記コンピュータに実行させ、

前記表示する機能は、検出された前記デジタル署名に関する情報を表示することを特徴とするコンピュータプログラム。

【請求項 9】

請求項 8 に記載のコンピュータプログラムにおいて、

前記デジタル署名に関する情報は、前記デジタル署名を施した主体に関する情報であることを特徴とするコンピュータプログラム。

【請求項 10】

請求項 8 または 9 のいずれかに記載のコンピュータプログラムにおいて、

前記表示する機能は、前記部分データの内容と前記デジタル署名に関する情報を関連付けて表示することを特徴とするデジタル署名検証装置。

【請求項 11】

請求項 1 0 に記載のコンピュータプログラムにおいて、

前記表示する機能は、前記部分データの内容を示す情報を他の情報と区別して表示することを特徴とするコンピュータプログラム。

【請求項 1 2】

請求項 7 乃至 1 1 のいずれかに記載のコンピュータプログラムにおいて、

前記デジタル署名は、XMLにより記述され、

前記検知する手段は、所定のデータを指し示すものであって、XMLにより規定された前記識別子を検索し、検索された前記識別子に基づいて検知することを特徴とするコンピュータプログラム。

【請求項 1 3】

電子データに対して、デジタル署名を施すデジタル署名データ作成装置において、

プログラムが格納された記憶装置と、

前記記憶装置と接続され、前記プログラムに従って、前記電子データに含まれる部分データに対しデジタル署名を施し、前記部分データを特定する識別子を生成し、前記デジタル署名が施された部分データおよび前記識別子を含むデジタル署名データを作成する処理装置を備えたことを特徴とするデジタル署名データ作成装置。

【請求項 1 4】

請求項 1 3 に記載のデジタル署名データ作成装置において、

前記処理装置と接続され、ネットワークを介して情報処理装置と接続され、前記ネットワークを介して前記情報処理装置へ、作成された前記デジタル署名データを送信するネットワーク接続装置を、さらに備えたことを特徴とするデジタル署名データ作成装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル署名を検証する技術に関する。より詳しくは、少なくともひとつのデジタル署名されたデータを表示することが可能な技術に関する。

【0002】

【従来の技術】

官公庁や自治体、民間企業などの組織体の中で取り交わされる契約書などの書類に対して、紙によるやり取りに代えてコンピュータ等の情報処理装置を利用して作成した電子文書によるやり取りをすることが増えている。この電子文書のやり取りに当たり、本人性の保証や他者等による改ざんの防止のために電子的な署名（デジタル署名）が利用されつつある。デジタル署名自体の技術については、たとえば「デジタル署名と暗号技術」1997年刊（ピアソン・エデュケーション）P90～95に記載されている。

【0003】

また、デジタル署名されたデータに対してさらにデジタル署名を行う多重署名や、データの特定の部分にのみデジタル署名を行う部分署名の方式も種々提案されている。それらを活用して複数のデジタル署名が可能である。

【0004】

デジタル署名されていることを表示する方法としては、たとえば「Webセキュリティ&コマース」1998年刊（オライリー・ジャパン）P173～183に記述されているAuthenticode技術がある。本技術は、署名を検出すると証明書を表示する方式である。また、多重署名の状態を表示する技術としては、特開平2000-293102「デジタル多重署名装置および記憶媒体」で示される多重署名装置がある。

【0005】

【発明が解決しようとする課題】

しかしながら、上述の公知例ではデジタル署名されていることを表示する際に、署名対象のデータに関する情報としてファイル名しか表示されないため。このために、署名対象のデータの内容をすぐに確認することが出来ないという問題がある。

【0006】

また、近年注目されているXML（eXtensible Markup Language）文書には、ファイル中の一部分を署名対象として指定した部分署名が可能である。しかし、

ファイル全体に対するデジタル署名を想定とした上述の従来技術では、部分署名とその署名対象のデータの内容をすぐに確認することは困難であった。

【0007】

本発明では、デジタル署名とその署名対象となるデータ（ファイル）の内容を、容易に確認することを目的とする。

【0008】

【課題を解決するための手段】

上記の目的を達成するために本発明では、以下の構成をとる。

デジタル署名の対象となるデータと当該デジタル署名の対象となる範囲を示す情報を対応付けるものである。ここで、デジタル署名の対象となるデータは、所定の単位中の部分データであってもよい。所定の単位の1例としては1つのファイルがある。

【0009】

本発明には、以下の構成も含まれる。

デジタル署名の対象となる範囲を示す情報として、デジタル署名対象データ識別子を、デジタル署名ファイルに添付することが含まれる。また、入力されるデジタル署名ファイルに添付されたデジタル署名対象データ識別子に基づいて、デジタル署名の対象となる範囲（部分データ）を検知する。デジタル署名の対象となる範囲の検知には、デジタル署名ファイルを解析し、どのようなデータが含まれるかを検知することが含まれる。

【0010】

これらの処理の結果に基づいて、デジタル署名の対象となる範囲の内容とデジタル署名に関するデータを関連付けて表示することも、本発明に含まれる。デジタル署名に関するデータには、デジタル署名を行った装置もしくは利用者に関する情報が含まれる。また、関連付けた表示としては、同じディスプレイ上に表示することが含まれる。

【0011】

【発明の実施の形態】

以下に、デジタル署名の表示を行う実施形態におけるデジタル署名表示装置に

ついて説明する。

図2は、本実施形態のデジタル署名表示装置の概略構成を示す図である。図2に示すように本実施形態のデジタル署名表示装置は、CPU201とメモリ202と、磁気ディスク装置203と、入力装置204と、ディスプレイ装置205と、ネットワーク接続装置206とを有している。

【0012】

CPU201は、デジタル署名表示装置全体の動作、処理を制御するものである。メモリ202は、デジタル署名表示装置全体の動作を制御する際に、その為の各種処理プログラムやデータをロードする記憶装置である。

【0013】

磁気ディスク装置203は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置204は、デジタル署名表示装置への操作指示等を入力する装置である。ディスプレイ装置205は、デジタル署名表示装置の動作状況や、デジタル署名状況を表示する装置である。ネットワーク接続装置206は、デジタル署名表示装置をネットワークに接続し、ネットワークに接続されたほかの装置とデータのやり取りを行う装置である。

【0014】

また、デジタル署名表示装置は、デジタル署名解析処理部210とデジタル署名表示画面生成処理部211を有している。

【0015】

デジタル署名解析処理部210は、入力装置204によって指定されたデジタル署名ファイルを入力し、デジタル署名の対象となるデータや、デジタル署名の有効性の検証、デジタル署名者等の情報を解析し、解析結果を出力する処理部である。

【0016】

デジタル署名表示画面生成処理部211は、前記デジタル署名解析処理部210の出力した解析結果を入力し、デジタル署名表示画面を生成しディスプレイ装置205に表示する処理を行う処理部である。

【0017】

デジタル署名表示装置をデジタル署名解析処理部 2 1 0 およびデジタル署名表示画面生成処理部 2 1 1 として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記憶媒体はCD-ROM以外の他の記録媒体でも良い。また、プログラムは、ネットワークを介して配信されてもよい。

【 0 0 1 8 】

デジタル署名は、たとえば標準化団体であるW3Cによって策定中の、XML-Signatureという仕様を用いてもよい。図5に、XMLに準拠したデジタル署名ファイルの例 `dsign.xml` を示す。本デジタル署名ファイルは、タグ<Signature>から</Signature>までの001行目から023行目でデジタル署名情報を示す。005行目のタグ<Reference>中で指定されている署名対象データ識別子501「ALL」は、署名対象データを識別する識別子である。前記識別子501「ALL」の示すデータは、本デジタル署名ファイル中の024行目のタグ<Object Id="ALL">から047行目の</Object>で囲まれる部分である。

【 0 0 1 9 】

図3は、本実施形態におけるデジタル署名表示装置のデジタル署名解析処理部210の処理手順を示すフローチャートである。図3に示すようにデジタル署名解析処理部210は、入力装置204から入力される、デジタル署名ファイル名を入力し、デジタル署名を解析する処理を行う。

【 0 0 2 0 】

以下、図5に示すデジタル署名ファイル `dsign.xml` が指定された場合を例に処理を説明する。

ステップ301で前記指定された図5に示すデジタル署名ファイル `dsign.xml` を、磁気ディスク装置203から読み込み、ファイルからデジタル署名を検索する。本実施形態では、タグ<Signature>と</Signature>で囲まれるデータを検索することでデジタル署名の存在を認識する。

【 0 0 2 1 】

ステップ302では、前記指定されたデジタル署名ファイル中にデジタル署名

が存在しないか、もしくは解析済みのデジタル署名しか存在しない場合は、処理を終了する。解析していないデジタル署名が検出されたら、ステップ 3 0 3 に進む。

【 0 0 2 2 】

ステップ 3 0 3 では、検出されたデジタル署名を解析し、デジタル署名対象データを検索する。図 5 のデジタル署名ファイルでは、0 0 4 行目の<Reference IDREF="ALL">タグに示されるデジタル署名対象データ識別子“ALL”が示すデータを検索する。検索の結果、デジタル署名ファイル中の 0 2 3 行目<Object ID="ALL">から 0 4 7 行目</Object>が署名対象データであると認識する。ここで、識別子は特定のデータを指し示すデータであり、識別子の示すデータが前記デジタル署名ファイルの外部であってもかまわない。その場合、デジタル署名対象データ識別子はたとえば U R I 形式で表記する。

以降、デジタル署名対象データが含まれるファイルをデジタル署名データファイルと呼ぶ。

【 0 0 2 3 】

ステップ 3 0 4 では、デジタル署名の検証を行い、デジタル署名が正当なものであるかどうかを判定するとともに、署名作成者の情報を取得する。図 5 のデジタル署名ファイル d s i g n . x m l では、0 1 6 行目<X509Name></X509Name>タグによっては含まれる部分「CN=Tomita Taminori,O=Hitachi,C=JP」に署名作成者の情報が記述されている。

【 0 0 2 4 】

ステップ 3 0 5 では、ステップ 3 0 3 で確定した、前記デジタル署名対象データの領域と、デジタル署名対象データファイル名と、ステップ 3 0 4 で取得した署名作成者、署名検証結果をデジタル署名解析結果として出力する。

【 0 0 2 5 】

図 6 に、デジタル署名解析結果の例を示す。図 6 に示すように、デジタル署名ファイル名、署名作成者情報、デジタル署名対象データファイル名、署名対象データ識別子、署名検証結果から構成される。

【 0 0 2 6 】

デジタル署名解析結果出力後、再びステップ302に戻り、未解析のデジタル署名が存在する場合は、ステップ303からステップ305を繰り返す。デジタル署名ファイル中に存在するデジタル署名の解析を完了したら、処理を終了する。処理の終了は、対象となるデジタル署名全ての解析の完了を条件としてもよい。

【0027】

デジタル署名解析処理部210の処理終了後、デジタル署名表示画面生成処理部211の処理が開始される。図4に示すようにデジタル署名表示画面生成処理部211は、前記デジタル署名解析処理部210が出力した、デジタル署名解析結果を入力し、デジタル署名対象を表示する画面を生成する処理を行う。

【0028】

ステップ401では、前記デジタル署名解析処理部の出力した、前記デジタル署名解析結果を入力する。

【0029】

ステップ402では、前記デジタル署名解析結果に未表示のデジタル署名解析結果が存在しない場合は、処理を終了する。表示していないデジタル署名が存在する場合は、ステップ403に進む。

【0030】

ステップ403では、前記未表示のデジタル署名解析結果に示される、デジタル署名対象データファイルを表示する。既に前記デジタル署名対象データファイルが表示されている場合は、本処理は省略する。図6の例におけるデジタル署名対象データファイルdesign.xmlの表示例を、図7に示す。

【0031】

ステップ404では、ステップ403で表示されたデジタル署名対象データファイルのうち、デジタル署名対象データの領域を示す枠を生成する。図6の例における表示例を、図8に示す。図中101はデジタル署名対象データの領域を示す枠である。

【0032】

ステップ405では、ステップ404で表示された、前記デジタル署名対象デ

一タの領域を示す枠が示すデジタル署名の署名解析結果を表示する。図6の例における表示例を図1に示す。図中101はデジタル署名対象データの領域を示す枠、102は前記枠101が示すデジタル署名の解析結果の表示である。

【0033】

署名解析結果の表示方法は、図1に示したように文字列で表示する以外にも、色や、記号で表示してもよい。

また、たとえば前記表示枠101の色によって、署名検証結果を表現することにしても良い。

【0034】

ステップ405終了後、再びステップ402に戻り、未表示のデジタル署名解析結果が存在する場合は、ステップ403からステップ405を繰り返す。デジタル署名解析結果の画面生成を完了したら、処理を終了する。処理の終了は、全てのデジタル署名解析結果の画面生成を完了したことを条件としてもよい。

【0035】

以上説明したように、本実施形態のデジタル署名表示装置によれば、デジタル署名者の情報と、その署名対象のデータの内容を一つの画面上に表示するためどのような内容が、何者によってデジタル署名されているのかを多くの操作なしに確認することができる。

【0036】

なお、本実施形態ではデジタル署名解析処理部210と、デジタル署名表示画面生成処理部211が、同一の装置で実現されているが、それぞれ別の装置で実現されてもかまわない。

【0037】

図9は、XMLによって記述された第二のデジタル署名ファイルd s i g n 2 . x m l の例である。

【0038】

第二のデジタル署名ファイルはタグ<Signature>から</Signature>までの002行目から023行目までの第一のデジタル署名901と、024行目から045行目までの第二のデジタル署名903を含む。

【 0 0 3 9 】

図 9 中 タグ 署名 対象 データ 識別 子 9 0 2 は、第一のデジタル署名 9 0 1 の署名対象データを識別する識別子である。識別子 9 0 2 は、タグ<Reference>中で指定されている。識別子 9 0 2 の示すデータは、図 5 のファイル d s i g n . x m l 中の 0 2 5 行目のタグ<Object Id="author">から 0 3 3 行目の</Object>で囲まれる部分である。なお、識別子 9 0 2 は、具体的な例としては、" http://home/dsign.html#author "がある。

【 0 0 4 0 】

同様に、図 9 の署名対象識別子 9 0 4 は、第二のデジタル署名 9 0 3 の署名対象データを識別する識別子である。署名対象識別子 9 0 4 の示すデータは、図 5 のファイル d s i g n . x m l 中の 0 3 4 行目のタグ<Object Id="title">から 0 4 5 行目の</Object>で囲まれる部分である。なお、署名対象識別子 9 0 4 は、具体的な例としては、"http://home/dsign.html#title"がある。

【 0 0 4 1 】

このような第二のデジタル署名ファイルを、前記デジタル署名解析処理部 2 1 0 で処理した結果を図 1 0 に示す。

【 0 0 4 2 】

図 1 0 は、第二のデジタル署名ファイルのデジタル署名解析結果である。図中 1 0 0 1 は第一のデジタル署名 9 0 1 のデジタル署名解析結果、図中 1 0 0 2 は第二のデジタル署名 9 0 3 のデジタル署名解析結果である。

【 0 0 4 3 】

次に、図 1 0 に示すデジタル署名解析結果を、前記デジタル署名表示画面生成処理部 2 1 1 で処理し、デジタル署名表示画面を生成する。

【 0 0 4 4 】

図 1 1 に、第二のデジタル署名ファイルの表示画面例を示す。表示枠 1 1 0 1 は第一のデジタル署名 9 0 1 の署名対象範囲、署名情報 1 1 0 2 は第一のデジタル署名 9 0 1 の署名解析結果に関する情報である。同様に表示枠 1 1 0 3 は第二のデジタル署名 9 0 3 の署名対象範囲、署名情報 1 1 0 4 は第二のデジタル署名 9 0 3 の署名解析結果に関する情報である。

【0045】

以上説明したように、本実施形態のデジタル署名表示装置によれば、デジタル署名対象のデータがファイルの一部であっても、デジタル署名対象ファイルの内容と、デジタル署名対象の領域と、デジタル署名者の情報を一つの画面上に表示するためどのような内容が、何者によってデジタル署名されているのかを多くの操作なしに確認することができる。また一つの署名対象ファイルに対して複数の署名者が署名をした場合でも同様に多くの操作なしに確認することができる。

【0046】

図12は、XMLによって記述された第三のデジタル署名ファイル `dsign3.xml` の例である。

【0047】

第三のデジタル署名ファイルは002行目から018行目までの第一のデジタル署名1201と、020行目から036行目までの第二のデジタル署名1203を含む。

【0048】

前記第一のデジタル署名1201の署名対象データは019行目から049行目の識別子「ALL」で示される領域1202で、同様に前記第二のデジタル署名1203の証明対象データは037行目から048行目の識別子「title」で示される領域1204である。

【0049】

この第三のデジタル署名ファイルを、前記デジタル署名解析処理部210で処理した結果を図13に示す。

【0050】

図13は、第三のデジタル署名ファイルのデジタル署名解析結果である。図中1301は前記第一のデジタル署名1201のデジタル署名解析結果、図中1302は前記第二のデジタル署名1203のデジタル署名解析結果である。

【0051】

次に、図13に示すデジタル署名解析結果を、デジタル署名表示画面生成処理部211で処理し、デジタル署名表示画面を生成する。

【0052】

図14に、第三のデジタル署名ファイルの表示画面例を示す。表示枠1401は第一のデジタル署名1201の署名対象範囲、署名情報1402は第一のデジタル署名1201の署名解析結果に関する情報である。同様に表示枠1403は第二のデジタル署名1203の署名対象範囲、署名情報1404は第二のデジタル署名1203の署名解析結果に関する情報である。

【0053】

表示枠1401と、1403の包含関係から、第一のデジタル署名1201は識別子「title」で示される領域と、第二のデジタル署名1203を含めたデータに対する署名であることが容易に確認することができる。

【0054】

以上説明したように、本実施形態のデジタル署名表示装置によれば、デジタル署名対象のデータが複数のデジタル署名により多重署名されてあっても、デジタル署名対象の領域の包含関係によって、どのような内容が、何者によってデジタル署名されているのかを容易に確認することができる。

【0055】

なお、本発明による署名対象データの領域の表示方法は、上述した実施形態に限定されるものではない。たとえば、実施形態にあった枠線の代わりに、画面背景の表示色を変えて表示してもよい。

【0056】

また、本発明による署名情報の表示内容は、上述した実施形態に限定されるものではない。たとえば、実施形態の署名者情報および署名検証結果を表示してもよい。また、署名検証結果を表示してもよい。署名検証結果については、これを単独で表示してもよい。

【0057】

また、本発明によるデジタル署名方式は、上述した実施形態に限定されるものではない。すくなくとも署名対象データと署名者の情報を特定する情報を有するすべてのデジタル署名方式に適用可能である。

【0058】

すなわち、本発明は、デジタル署名を表現する手段において、デジタル署名されたデータを含むファイルの内容と、デジタル署名対象の領域と、署名情報を同一画面に表示する、という要旨を逸脱しない範囲で実施することができる。

【 0 0 5 9 】

また、本実施形態によれば、デジタル署名対象のデータを含むファイルの内容を表示し、その表示画面にデジタル署名対象の領域と、デジタル署名情報を二次元的に重ねて表示するので、部分署名、多重署名等の多様なデジタル署名の関係を、多くの操作なしに確認することが可能である。

【 0 0 6 0 】

【発明の効果】

本発明によれば、デジタル署名の対象となっているデータの内容を容易に把握することが可能になる。

【図面の簡単な説明】

【図 1】 本発明の実施形態のデジタル署名表示装置でデジタル署名データ `design.xml` を表示した図である。

【図 2】 本発明の実施形態のデジタル署名表示装置の概略構成を示す図である。

【図 3】 本発明の実施形態のデジタル署名解析処理部 210 の処理手順を示すフローチャートである。

【図 4】 本発明の実施形態のデジタル署名表示画面生成処理部 211 の処理手順を示すフローチャートである。

【図 5】 デジタル署名データ `design.xml` を示す図である。

【図 6】 デジタル署名データ `design.xml` をデジタル署名解析処理部 210 で処理した結果得られた、デジタル署名情報の例を示す図である。

【図 7】 デジタル署名データ `design.xml` の表示例を示す図である。

【図 8】 デジタル署名データ `design.xml` の表示例に、識別子 `ALL` で示されるデータを示す枠を表示した図である。

【図 9】 デジタル署名データ `design2.xml` を示す図である。

【図 10】 デジタル署名データ `design2.xml` をデジタル署名解析処理部 210 で処理した結果得られた、デジタル署名情報の例を示す図である。

【図 1 1】 本発明の実施形態のデジタル署名表示装置でデジタル署名データ d s i g n 2 . x m l を表示した図である。

【図 1 2】 デジタル署名データ d s i g n 3 . x m l を示す図である。

【図 1 3】 デジタル署名データ d s i g n 3 . x m l をデジタル署名解析処理部 2 1 0 で処理した結果得られた、デジタル署名情報の例を示す図である。

【図 1 4】 本発明の実施形態のデジタル署名表示装置でデジタル署名データ d s i g n 3 . x m l を表示した図である。

【符号の説明】

1 0 1 …デジタル署名対象データの領域を示す枠、 1 0 2 …デジタル署名データ d s i g n . x m l における署名解析結果に関する情報の表示、 2 1 0 …デジタル署名解析処理部、 2 1 1 …デジタル署名表示画面生成処理部、 1 1 0 1 …デジタル署名データ d s i g n 2 . x m l における第一のデジタル署名対象データの領域を示す枠、 1 1 0 2 …デジタル署名データ d s i g n 2 . x m l における第一の署名解析結果に関する情報の表示、 1 1 0 3 …デジタル署名データ d s i g n 2 . x m l における第二のデジタル署名対象データの領域を示す枠、 1 1 0 4 …デジタル署名データ d s i g n 2 . x m l における第二の署名解析結果に関する情報の表示、 1 4 0 1 …デジタル署名データ d s i g n 3 . x m l における第一のデジタル署名対象データの領域を示す枠、 1 4 0 2 …デジタル署名データ d s i g n 3 . x m l における第一の署名解析結果に関する情報の表示、 1 4 0 3 …デジタル署名データ d s i g n 3 . x m l における第二のデジタル署名対象データの領域を示す枠、 1 4 0 4 …デジタル署名データ d s i g n 3 . x m l における第二の署名解析結果に関する情報の表示

【書類名】 図面

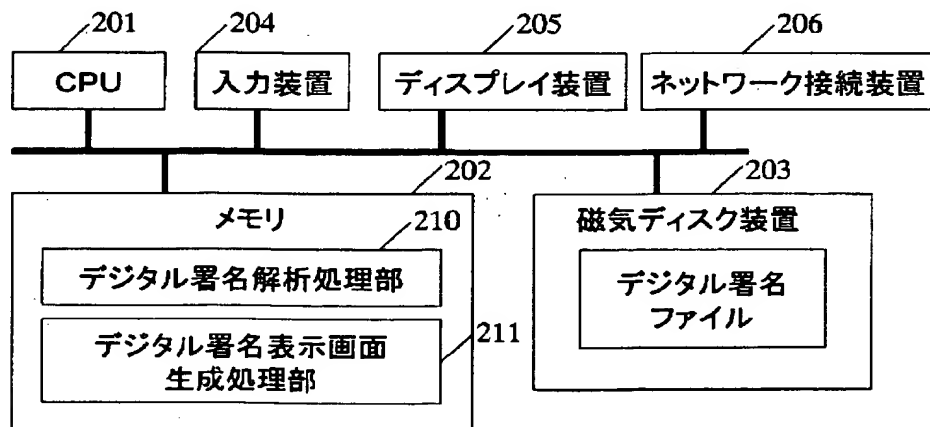
【図 1】

図 1

<p>著者 Tamimori Tomita 国籍 Japan 生年 1969 没年 ----</p> <p>【要約】</p> <p>【課題】</p> <p>デジタルコンテンツの不正使用を防止することが可能な技術を提供する。</p> <p>【解決手段】</p> <p>デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、 当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、 前記設定された状態情報の値に応じて、 当該デジタルコンテンツの再生処理を制御するステップとを有するものである。</p>	101
署名者情報:CN=Tomita Tamimori, O=Hitachi, C=JP 検証結果:OK	102

【図 2】

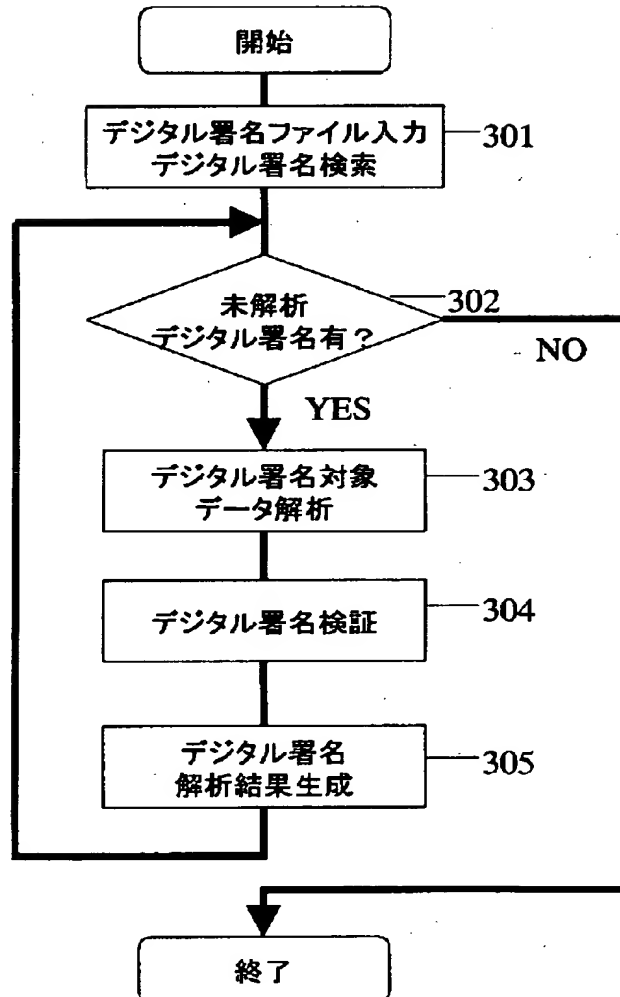
図 2



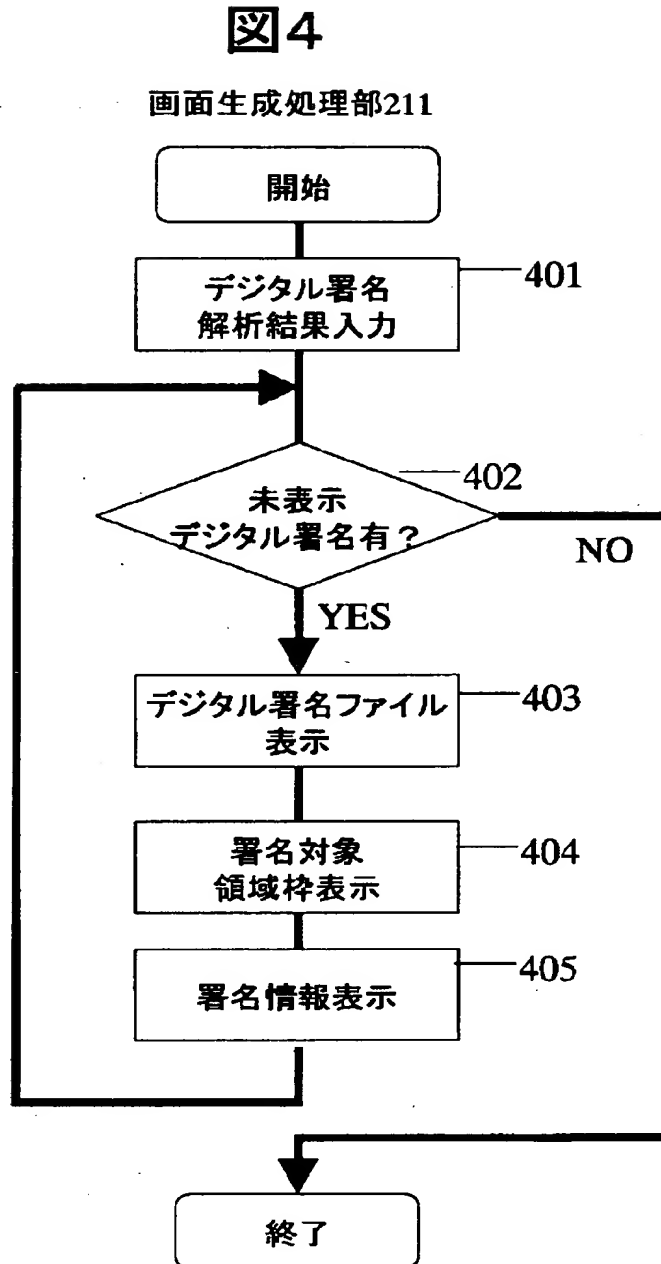
【図3】

図3

デジタル署名解析処理部210



【図4】



【図5】

図5

```

                                dsign.xml
001 <document>
002   <Signature>
003     <SignedInfo>
004       <SignatureMethod Algorithm="http://. . ."/>
005       <Reference IDREF="ALL">
006         <DigestMethod Algorithm="http://. . ."/>
007         <DigestValue Encoding=". . .">
008           WFKRfGWiAni9bY9k/sXgBft4ge4=
009         </DigestValue>
010       </Reference>
011     </SignedInfo>
012     <SignatureValue>
013       MCwCFBOM62GxrrxMGm7qfBt8R+Zv4YuIAhRvQH1DkgAdtnDQIOYog07srWha1A==
014     </SignatureValue>
015     <KeyInfo>
016       <X509Data>
017         <X509Name>CN=Tomita Taminori, O=Hitachi, C=JP</X509Name>
018         <X509Certificate>
019 tLKJqNhJznnUvkqZQ2ce+6slaulJ8cw7yALDZJhzfFlhHzALBgcqhkJOOAQDBQADLwAwLAIUZUJD
020         </X509Certificate>
021       </X509Data>
022     </KeyInfo>
023   </Signature>
024   <Object ID="ALL">
025     <Object Id="author">
026       <author>
027         <last-name>Tomita</last-name>
028         <first-name>Taminori</first-name>
029         <nationality>Japan</nationality>
030         <year-of-birth>1969</year-of-birth>
031         <year-of-death>----</year-of-death>
032       </author>
033     </Object>
034     <Object Id="tilte">
035       <title>【要約】</title>
036       <lines>
037         <line>【課題】
038         <line>デジタルコンテンツの不正使用を防止することが可能な技術を提供する。</line>
039         <line>【解決手段】</line>
040         <line>デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、</line>
041         <line>当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、</line>
042         <line>前記設定された状態情報の値に応じて、</line>
043         <line>当該デジタルコンテンツの再生処理を制御するステップとを有するものである。</line>
044       </lines>
045     </Object>
046   </Object>
047 </document>

```

【図 6】

図 6

#	デジタル署名 ファイル名	署名者作成者情報	デジタル署名対象 データファイル名	署名対象データ 識別子	署名検証結果
1	dsign.xml	CN=Tomita Taminori, O=Hitachi, C=JP	dsign.xml	ALL	OK

【図 7】

図 7

著者 Taminori Tomita
 国籍 Japan
 生年 1969
 没年 ----

【要約】

【課題】

デジタルコンテンツの不正使用を防止することが可能な技術を提供する。

【解決手段】

デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、
 当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、
 前記設定された状態情報の値に応じて、
 当該デジタルコンテンツの再生処理を制御するステップとを有するものである。

【図 8】

図 8

著者 Taminori Tomita
国籍 Japan
生年 1969
没年 —

【要約】

【課題】

デジタルコンテンツの不正使用を防止することが可能な技術を提供する。

【解決手段】

デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、前記設定された状態情報の値に応じて、当該デジタルコンテンツの再生処理を制御するステップとを有するものである。

—101

【図 9】

図 9

dsign2.xml

```

001 <document>
002   <Signature>
003     <SignedInfo>
004       <SignatureMethod Algorithm="http://..."/>
005       <Reference IDREF="http://home/dsign.html#author">
006         <DigestMethod Algorithm="http://..."/>
007         <DigestValue Encoding="...">
008           bY3JsOGI6Nd6ddsafT9FAn++2uK9gBft4ge4=
009         </DigestValue>
010       </Reference>
011     </SignedInfo>
012     <SignatureValue>
013       4eX1QCDRKrxFr/bY3JsOGI6Nd6afT9FAn++2uK9yWegTSmM6aiAqmb0Eiybf50q7d
014     </SignatureValue>
015     <KeyInfo>
016       <X509Data>
017         <X509Name>CN=Taminori Tomita, C=JP</X509Name>
018         <X509Certificate>
019 tLKvkqZQ2ce+6slaulJ6slaulJ8cw7yALDZJhzfFlhHzALBgcqhkjwLAIUZUJD
020         </X509Certificate>
021       </X509Data>
022     </KeyInfo>
023   </Signature>
024   <Signature>
025     <SignedInfo>
026       <SignatureMethod Algorithm="http://..."/>
027       <Reference IDREF="http://home/dsign.html#title">
028         <DigestMethod Algorithm="http://..."/>
029         <DigestValue Encoding="...">
030           hkjOOAQDBQADLwAwLAIUZUJD++2uK9gBft4ge4=
031         </DigestValue>
032       </Reference>
033     </SignedInfo>
034     <SignatureValue>
035       6slaulJ8cw7yALDZJhzfFlhHzALBgcqhkjOOAQDBQADLwAwLAIUZUJDAqmb0Eiybf50q7d
036     </SignatureValue>
037     <KeyInfo>
038       <X509Data>
039         <X509Name>CN=Taro Yamada, O=Hitachi syuppann, C=JP</X509Name>
040         <X509Certificate>
041 Ydoysr2usleZ9p6xRwEZYnoCFC97/v+w6FIyM+KgDDAgK9LYxN/n
042         </X509Certificate>
043       </X509Data>
044     </KeyInfo>
045   </Signature>
046 </document>

```


【図 1 0】

図10

#	デジタル署名 ファイル名	署名者作成者情報	デジタル署名対象 データファイル名	署名対象データ 識別子	署名検証結果	
1001	1	dsign2.xml	CN=Taminori Tomita, C=JP	dsign.html	http://home /dsign.html #author	OK
1002	2	dsign2.xml	CN=Taro Yamada, O=Hitachi syuppann, C=JP	dsign.html	http://home /dsign.html #title	OK

【図 1 1】

図11

著者 Taminori Tomita 国籍 Japan 生年 1969 没年 ----	1101
署名者情報: CN=Taminori Tomita, C=JP 検証結果: OK	1102
【要約】 【課題】 デジタルコンテンツの不正使用を防止することが可能な技術を提供する。 【解決手段】 デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、 当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、 前記設定された状態情報の値に応じて、 当該デジタルコンテンツの再生処理を制御するステップとを有するものである。	1103
署名者情報: CN=Taro Yamada, O=Hitachi syuppann, C=JP 検証結果: OK	1104

【図 12】

図12

design3.xml

```

001 <document>
002   <Signature>
003     <SignedInfo>
004       <SignatureMethod Algorithm="http://..."/>
005       <Reference IDREF="ALL">
006         . . .
007       </Reference>
008     </SignedInfo>
009     <SignatureValue>
010       MCwCFBOM62GxrrxMGm7qfBt8R+6slaulJ8cw7yALDZJhzfF1Og07srWhaiA==
011     </SignatureValue>
012     <KeyInfo>
013       <X509Data>
014         <X509Name>CN=Taro Yamada, O=Hitachi syuppann, C=JP</X509Name>
015       . . .
016       </X509Data>
017     </KeyInfo>
018   </Signature>
019   <Object ID="ALL">
020     <Signature>
021       <SignedInfo>
022         <SignatureMethod Algorithm="http://..."/>
023         <Reference IDREF="tilte">
024           . . .
025         </Reference>
026       </SignedInfo>
027       <SignatureValue>
028         MCwCFBOM62GxrrxMGm7qfBt8R+Zv4YuIAhRvQHQIOYOgO
029       </SignatureValue>
030       <KeyInfo>
031         <X509Data>
032           <X509Name>CN=Taminori Tomita, C=JP</X509Name>
033         . . .
034         </X509Data>
035       </KeyInfo>
036     </Signature>
037   </Object ID="tilte">
038     <title>【要約】</title>
039     <lines>
040       <line>【課題】
041       <line>デジタルコンテンツの不正使用を防止することが可能な技術を提供する。</line>
042       <line>【解決手段】</line>
043       <line>デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、</line>
044       <line>当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、</line>
045       <line>前記設定された状態情報の値に応じて、</line>
046       <line>当該デジタルコンテンツの再生処理を制御するステップとを有するものである。</line>
047     </lines>
048   </Object>
049 </Object>
050 </document>

```

1201

1202

1203

1204

【図 13】

図13

#	デジタル署名 ファイル名	署名者作成者情報	デジタル署名対象 データファイル名	署名対象データ 識別子	署名検証結果
1301 1	dsign3.xml	CN=Taro Yamada, O=Hitachi syuppann, C=JP	dsign3.html	ALL	OK
1302 2	dsign3.xml	CN=Taminori Tomita, C=JP	dsign3.html	title	OK

【図 14】

図14

【要約】

【課題】

デジタルコンテンツの不正使用を防止することが可能な技術を提供する。

【解決手段】

デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、前記設定された状態情報の値に応じて、当該デジタルコンテンツの再生処理を制御するステップとを有するものである。

署名者情報: CN=Taminori Tomita, C=JP 検証結果: OK

署名者情報: CN=Taro Yamada, O=Hitachi syuppann, C=JP 検証結果: OK

【書類名】 要約書

【要約】

【課題】

デジタル署名と署名対象データの内容の関係を容易に確認することが可能な装置を提供する。

【解決手段】

本発明のデジタル署名装置は、少なくとも署名対象のデータを識別する情報と、署名者を識別する情報が含まれるデジタル署名を含むファイルを入力し、前記デジタル署名と、前記デジタル署名の署名対象データの内容とを解析し、署名の検証を行い、それらの署名解析結果を出力するデジタル署名解析手段と、前記署名対象データの内容と、前記署名解析結果を合わせて表示するデジタル署名表示画面を生成するデジタル署名表示画面生成手段とを備えるものであり、前記デジタル署名表示画面は署名対象データの内容とデジタル署名の情報を同一画面上に表示する。

【選択図】 図 2

認定・付加情報

特許出願の番号	特願2001-136827
受付番号	50100657189
書類名	特許願
担当官	第七担当上席 0096
作成日	平成13年 5月 9日

<認定情報・付加情報>

【提出日】	平成13年 5月 8日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所